EXHIBIT T to Amendment No. 60

ADDENDUM 12 TO APPENDIX 8 TO SCHEDULE 3.3 TO THE COMPREHENSIVE INFRASTRUCTURE AGREEMENT

SECURE WIRELESS NETWORK SERVICES

EXHIBIT T to Amendment No. 60

Overview

Secure Wireless Network Services are based on the IEEE 802.11 set of standards and meet the Commonwealth of Virginia (CoV) ITRM Standard SEC 501-01. This service, available via the new MPLS network, will provide secure connectivity to the VITA network from 802.11 wirelessly enabled desktop, laptop, and tablet workstations and Personal Digital Assistants (PDAs). The service provides secure wireless 802.11A/B/G access for Commonwealth users and guests (if requested) within the designated areas of a facility requesting this service. This secure wireless infrastructure will provide security and network management for the secure wireless systems. Secure Wireless Network Service is intended to be a convenience service and additional to standard Data Network Services.

Technical Description

With Secure Wireless Network Service, the Commonwealth can securely connect users with wireless-capable devices to a local-area-network (LAN) using encryption and authentication technologies that protect data from unauthorized use. The Secure Wireless Network Service provides the following:

Mobility

- Within the work place, provides secure wireless authenticated access to the network and to applications requiring network access.
- Gives users the ability to work independently without having to be plugged into work areas such as conference rooms or other joint meeting areas where there are not enough outlets for users to plug into.
- Option for guest access to the Internet via the Guest VLAN to check mail or browse the web.

Security

- Users authenticate against [redacted]
- Encryption –data is encrypted over the secure wireless network.
- Theft of access points will not compromise network due to the fact that they receive their information via their controllers.

Monitoring

- [redacted]
- [redacted].

Technical Solution

Secure Wireless Site Survey

Vendor will conduct a wireless survey of the applicable Eligible Customer Location. The intent of this survey is to assess the impact of the Eligible Customer Location's construction and layout on the theoretical performance of the secure wireless network. Based on the results of this survey, Vendor will recommend the quantity and location of the secure wireless access points to VITA and the Eligible Customer.

Components

The solution consists of three components as follows:

- [redacted]
  - [redacted]
  - [redacted]
- [redacted]
  - [redacted]
  - [redacted]
- [redacted]
  - [redacted]
  - [redacted]

[redacted]

Architecture

The 802.11 secure wireless devices for End-Users and guests will be housed at the Eligible Customer Locations.
The users are categorized as two distinct types defined as follows:

- Category 1 - End-Users
- Category 2 – guest users

The Secure Wireless Network Service consists of the physical secure wireless access media [redacted] and core components for secure wireless intrusion detection and prevention, and Network Management [redacted]

The secure wireless system will provide a framework for ensuring that each user can only access those tools and services defined by their network access rights. The secure wireless design provides secure wireless 802.11 A/B/G access for End-Users and guests users within the Eligible Customer Locations. Secure wireless access is provided throughout the requested areas of coverage within the facility. The access points are mounted to or above the ceiling tiles or to the drop ceiling grids through out the Eligible Customer Location(s).

Vendor's secure wireless data solution architecture is shown in the following Figures 1 and 2 below:

Figure 1 - REDACTED

Figure 2 - REDACTED

Vendor will install the WAPs as dictated by the wireless site survey in conjunction with the Eligible Customer's business requirements. The WAPs are connected to the on-site switch via customer-provided Category 5 (CAT5e) or better ethernet cabling, thus additional ports on the LAN switches must be available. The cabling used for the secure wireless solution must meet Vendor's cabling standards to support Power over Ethernet (PoE) usage. [redacted] This architecture will allow the Vendor to remotely monitor and manage the entire secure wireless infrastructure from the ENOC at CESC.

Vendor's architecture provides two connectivity paths depending on the category of user. End-Users can authenticate to [redacted] and have full network access after successful authentication. Users who do not have [redacted] are segregated to the Guest VLAN that only provides Internet access through the Internet Secure Gateway (ISG).

Security / Authentication

Vendor's Secure Wireless Network Service was developed specifically to meet the security requirements provided by VITA. The solution includes the following security functionality:

- [redacted]Requires End-Users to utilize [redacted]
- Guests accessing the secure wireless network are directed to the Internet through the Internet Secure Gateway (ISG) [redacted]
- [redacted].
- Communication between the user devices and the WAPs utilize the advanced protocol WPA2 and is certified by the Wi-Fi Alliance. WPA2 introduces the use of AES-based encryption algorithms.
- A unique Service Set Identifier (SSID) will be established in the WLAN device, but will not be broadcasted.

[redacted]

Technical Assumptions

Vendor's Secure Wireless Network Service includes the following assumptions:

- Adequate ports on the LAN switches must be available.

[redacted]

- Users who do not have CoV network rights are considered "guest users" and will be segregated to the Guest VLAN that only provides internet access through the enterprise Internet Secure Gateway (ISG).
- The wireless network interface cards on the user devices must be configured for Wi-Fi Protected Access 2 (WPA2) mode. Vendor's standard PC images include this capability.; otherwise Vendor is not responsible for Wi-Fi capabilities at the user level (e.g., desktop, laptop, and tablet workstations and PDAs) under this SOW.
- The user device must be configured to disable the secure wireless interface when a wired connection is present to eliminate unwanted wireless bridging to the wired network.
- The site where secure wireless network is installed must have completed network transformation and have access to the MPLS network back to CESC.
- The site where secure wireless network is installed must have completed messaging transformation and have access to the COVA Common Domain.

[redacted] The site where secure wireless network access is installed must have completed [redacted]

- If all assumptions are not met there may be latency issues as well as bandwidth constraints that could arise due to additional traffic overhead.
- Vendor is not responsible for identifying guest users.